SCNR Government College, Proddatur
SKILL COURSE
w.e.f. AY 2023-24
SEMESTER-IV
CYBER SECURITY

UNIT - I: Introduction to Cybercrime: Introduction, Cybercrime: Definition and origins of the word, Cybercrime and Information Security, who are cyber criminals? classifications of cybercrimes, cybercrime: the legal perspectives, an Indian perspective, cybercrime and the Indian IT Act 2000, a Global perspective on Cybercrimes.

UNIT - I:

Cybercrime: Definition & Origins:

Definition: Cybercrime is illegal activity involving computers or networks, including hacking, fraud, and data breaches. It can be committed by individuals, groups, or nation-states for financial gain, espionage, or disruption.

Examples of Cybercrime:

- Hacking into systems to steal data
- Spreading viruses or malware
- Online scams and fraud
- Attacks on government or corporate networks

Origins of the Word "Cybercrime": The term "cybercrime" **comes from two words:**

- **"Cyber"** – Derived from **"cybernetics"**, which relates to computers and digital technology.
- **"Crime"** – Any illegal act or offense.

The word **cybernetics** was first used in the 1940s, but **cybercrime** became popular in the 1990s when the internet became widely used.

Cybercrime & Information Security

Cybercrime refers to illegal activities involving computers, networks, or digital systems, such as hacking, fraud, identity theft, and ransomware attacks. It threatens individuals, businesses, and governments worldwide.

Information Security:
Information security (InfoSec) focuses on protecting digital and physical information from unauthorized access, theft, or damage.

It involves three key principles:

- **Confidentiality** – Ensuring only authorized people can access data.
- **Integrity** – Protecting information from being altered or corrupted.
- **Availability** – Ensuring data is accessible when needed.

Key Information Security Measures:

- **Firewalls & Antivirus** – Prevent unauthorized access and malware.
- **Encryption** – Securing data by converting it into unreadable formats.
- **Multi-Factor Authentication (MFA)** – Adding extra layers of security.
- **Regular Software Updates** – Patching vulnerabilities in systems.
- **Security Awareness Training** – Educating users on cyber threats.
- **Incident Response Plans** – Strategies to respond to cyberattacks.

Who Are Cybercriminals?

Cybercriminals are people who use computers and the internet to commit crimes. They can be individuals or groups and have different motives, such as stealing money, spying, or causing damage.

Types of Cybercriminals:

1. **Hackers** – Break into systems to steal data or cause harm.
2. **Scammers** – Trick people into giving money or personal information.
3. **Identity Thieves** – Steal personal details to commit fraud.
4. **Cyberterrorists** – Attack systems to create fear or chaos.
5. **Insider Threats** – Employees who misuse company data.
6. **Nation-State Attackers** – Government-backed hackers spying or disrupting other countries.

Classifications of Cybercrimes

Cybercrimes are criminal activities involving computers, networks, or digital devices. They can be classified based on their targets and nature.

1. Crimes Against Individuals: These crimes directly impact individuals by stealing their personal data or causing harm online.

- **Identity Theft** – Stealing personal details to commit fraud.
- **Online Scams & Fraud** – Tricking people into giving money or information.
- **Cyberstalking & Harassment** – Threatening or intimidating someone online.
- **Phishing** – Fake emails or messages to steal login details.

2. Crimes Against Organizations: Businesses and institutions are often targeted for financial gain or disruption.

- **Hacking & Data Breaches** – Unauthorized access to steal sensitive data.
- **Ransomware Attacks** – Locking systems and demanding payment to unlock them.
- **Denial-of-Service (DoS) Attacks** – Flooding a website to make it crash.
- **Insider Threats** – Employees misusing or leaking company data.

***3*. Crimes Against Governments:** Governments and critical infrastructure are targeted for espionage or disruption.

- **Cyber terrorism** – Online attacks to create fear or damage national security.

- **Espionage (Cyber Spying)** – Stealing government or military secrets.
- **Attacks on Critical Infrastructure** – Disrupting power grids, hospitals, or transportation systems.

4. Crimes Involving Digital Content: Illegal activities that involve harmful or banned digital content.

- **Child Exploitation & Abuse Materials** – Sharing illegal content involving minors.
- **Online Drug & Weapon Trafficking** – Selling illegal goods on the dark web.
- **Spreading Misinformation or Hate Speech** – Using fake news to manipulate or harm society.

Cybercrimes affect individuals, businesses, and governments worldwide. Understanding these classifications helps in developing better security measures and staying safe online.

The legal perspectives on cybercrime:

Cybercrime refers to offenses like hacking, identity theft, cyber fraud, and online harassment. Laws vary by country, with key regulations including:

- **CFAA (USA), Computer Misuse Act (UK), IT Act (India), GDPR (EU)** for data protection and cyber security.
- **Budapest Convention on Cybercrime (2001)**, the first international treaty for cybercrime cooperation.
- **Challenges:** Cybercrimes happen across different countries, making it hard to catch criminals. Government tracking can raise privacy concerns, and new dangers like AI scams and crypto currency fraud make things more complicated.
- **Prevention & Enforcement:** Groups like the FBI, Europol, and Interpol investigate cybercrimes using digital tools. Strong laws, public awareness, and good security practices help stop attacks.

An Indian perspective on Cyber Crime

With increasing digital adoption, India faces a rising threat of cybercrime, including financial fraud, hacking, ransomware, identity theft, cyber bullying, and misinformation.

Legal Framework & Government Initiatives:

- **IT Act, 2000** and **IPC Sections** address cyber offenses.
- **Personal Data Protection Bill** (upcoming) aims to regulate data security.
- **Cyber Surakshit Bharat, CERT-In, and Cyber Swachhta Kendra** enhance cybersecurity efforts.

Challenges:

- Low awareness and underreporting of cybercrimes.
- Jurisdictional issues and international cyber threats.
- Shortage of skilled cyber security professionals.

cybercrime and the Indian IT Act 2000

Cyber security in India requires a collective effort from the government, businesses, and individuals to ensure a safer digital future.

Cybercrime & IT Act 2000 (India):

Cybercrime includes hacking, identity theft, cyber stalking, and online fraud. India's **IT Act 2000**, amended in 2008, addresses these threats with key provisions:

- **Hacking & Data Theft (Sec. 43, 66)** – Penalizes unauthorized access.
- **Identity Theft (Sec. 66C, 66D)** – Covers digital impersonation.
- **Cyber Terrorism (Sec. 66F)** – Punishable by life imprisonment.
- **Obscene Content (Sec. 67)** – Regulates explicit material online.
- **Intermediary Liability (Sec. 79)** – Protects online platforms if they follow due diligence.

Challenges: Weak enforcement, jurisdictional issues, evolving threats like AI-driven cybercrimes, and lack of strong data protection laws.

Global Cybercrime Trends & Laws

Cybercrimes like **ransomware, AI-driven attacks, and data breaches** are rising. International frameworks include:

- **Budapest Convention (2001)** – First global treaty on cybercrime.
- **GDPR (EU)** – Strict data protection laws.
- **CFAA (USA)** – Criminalizes hacking.
- **China & Russia** – Strict cybersecurity laws for national security.

Global Challenges: Lack of universal laws, cross-border enforcement issues, and evolving cyber threats. Stronger **international cooperation** is needed to combat cybercrime effectively.

UNIT-II:

Cybercrime-Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Authentication Service Security, Attacks on Mobile/Cell Phones.

Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile Devices-Related Security Issues, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

UNIT-II

Cybercrime: Introduction, Proliferation of Mobile and Wireless Devices

The rapid growth of mobile and wireless technology has led to an increase in cybercrimes. As more people use smart phones, tablets, and other wireless devices for communication, banking, and online activities, cybercriminals exploit vulnerabilities to steal data, commit fraud, and disrupt services. Some common cybercrimes include:

- **Mobile Malware** – Viruses, spyware, and ransomware steal data or lock devices.
- **Phishing Attacks** – Fake messages trick users into sharing sensitive information.
- **Unsecured Wi-Fi Attacks** – Hackers intercept data on public networks.
- **SIM Swapping** – Attackers hijack phone numbers to access accounts.
- **Man-in-the-Middle Attacks** – Hackers intercept communications to steal or alter data.
- **Data Breaches** – Weak app security exposes sensitive information.
- **Bluetooth & NFC Exploits** – Attackers hack devices via wireless connections.
- **Social Engineering** – Scammers manipulate users into revealing personal data.

With more people relying on mobile technology, the risk of cybercrime increases. Taking security steps like using strong passwords, avoiding suspicious links, and updating devices can help prevent attacks.

Trends in Mobility

As mobile technology advances, new cyber threats emerge, targeting users and businesses. Some key cybercrimes linked to mobility trends include:

1. **App-Based Attacks** – Malicious apps steal data, track user activity, or spread malware.
2. **Cloud Security Breaches** – Increased mobile cloud usage makes data vulnerable to hacking.
3. **Mobile Payment Fraud** – Cybercriminals exploit digital wallets and mobile banking to steal money.
4. **IoT Device Exploits** – Weak security in smart devices leads to unauthorized access and data theft.
5. **BYOD (Bring Your Own Device) Risks** – Employees using personal devices for work increase security vulnerabilities.
6. **5G Network Attacks** – Faster, broader connectivity creates new entry points for hackers.
7. **AI-Powered Cyber Attacks** – Hackers use artificial intelligence to launch sophisticated phishing and malware campaigns.

As mobile technology evolves, strong security measures are essential to prevent cybercrime.

Syllabus: UNIT-II: Cybercrime-Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Authentication Service Security, Attacks on Mobile/Cell Phones.

Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile Devices-Related Security Issues, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

Introduction to Cybercrime in Mobile and Wireless Devices

Cybercrime involving mobile and wireless devices refers to illegal activities carried out using smartphones, tablets, laptops, and wireless networks such as Wi-Fi, Bluetooth, and cellular networks. With the widespread use of mobile devices for communication, banking, shopping, and social networking, attackers exploit vulnerabilities to steal data, commit fraud, and spread malware.

Proliferation of Mobile and Wireless Devices

The **proliferation of mobile and wireless devices** refers to the rapid increase in the number and usage of smartphones, tablets, laptops, wearable devices, and other wireless-enabled technologies. This growth has transformed the way people communicate, work, and access information.

Reasons for Proliferation

- **Affordable devices**: Reduced cost of smartphones and tablets
- **Advancement in wireless technologies**: 3G, 4G, 5G, Wi-Fi, and Bluetooth
- **Easy internet access**: Widespread availability of mobile data and hotspots
- **App ecosystem**: Mobile apps for banking, education, healthcare, and entertainment
- **Miniaturization of hardware**: Compact, powerful, and energy-efficient devices

Areas of Usage

- Communication (calls, messaging, video conferencing)
- Mobile banking and digital payments
- E-commerce and online services
- Education and e-learning
- Healthcare and fitness tracking
- Smart homes and Internet of Things (IoT)

Impact on Cybersecurity

- Increased exposure to **cyberattacks and data breaches**
- Greater risk of **malware, phishing, and identity theft**
- Security challenges due to **heterogeneous devices and operating systems**
- Difficulty in managing and securing personal and corporate data

Conclusion: The rapid proliferation of mobile and wireless devices has improved connectivity and convenience but has also created new cybersecurity challenges. Proper security measures, user awareness, and strong authentication mechanisms are essential to mitigate associated risks.

Trends in Mobility

Trends in mobility refer to the evolving ways in which mobile and wireless technologies are used to access information, services, and applications anytime and anywhere. These trends have reshaped business operations, communication, and daily life.

Major Trends in Mobility

1. **Bring Your Own Device (BYOD)**
   Employees use personal smartphones, tablets, and laptops for work, increasing flexibility but also raising security concerns.
2. **Mobile Cloud Computing**
   Data storage and processing are shifted to the cloud, enabling access from any mobile device with an internet connection.
3. **Mobile Payments and Digital Wallets**
   Use of mobile banking apps, UPI, NFC, and QR-code payments has increased cashless transactions.
4. **Location-Based Services (LBS)**
   Services like GPS navigation, ride-hailing apps, and location tracking rely on real-time user location data.
5. **High-Speed Wireless Networks**
   Adoption of 4G and 5G networks enables faster data transfer, low latency, and better mobile experiences.
6. **Internet of Things (IoT)**
   Integration of mobile devices with smart objects such as wearables, smart homes, and connected vehicles.
7. **App-Centric Computing**
   Increased dependence on mobile applications for communication, shopping, learning, and healthcare.

Conclusion

Trends in mobility enhance convenience and productivity but also introduce new cybersecurity risks. Effective security policies and user awareness are essential to ensure safe mobile computing.

Credit Card Frauds in the Mobile and Wireless Computing Era

The **mobile and wireless computing era** has made credit card usage more convenient through smartphones, mobile banking apps, and online payment platforms. However, this convenience has also increased **credit card frauds**, as cybercriminals exploit security weaknesses in mobile devices and wireless networks.

Common Types of Credit Card Frauds

1. **Phishing and Smishing**
   Fraudsters send fake emails or SMS messages pretending to be banks or service providers to steal card details, OTPs, or CVV numbers.
2. **Malicious Mobile Applications**
   Fake or infected apps capture card information entered by users and transmit it to attackers.

3. **Public Wi-Fi Attacks**
   Using unsecured Wi-Fi networks allows attackers to intercept card data through man-in-the-middle attacks.
4. **Mobile Malware and Spyware**
   Malware installed on smartphones records keystrokes, screenshots, or payment details.
5. **Fake Payment Links and QR Codes**
   Users are tricked into scanning fraudulent QR codes or clicking malicious payment links.
6. **SIM Swapping Attacks**
   Attackers take control of a victim's mobile number to receive OTPs and complete card transactions.

Prevention Measures

- Use trusted and official mobile applications
- Avoid public Wi-Fi for financial transactions
- Enable two-factor authentication
- Regularly monitor bank statements
- Install security updates and antivirus software

Conclusion: Credit card frauds in the mobile and wireless computing era pose serious financial and privacy risks. Strong security measures, secure mobile practices, and user awareness are crucial to preventing such frauds.

Authentication Service Security

Authentication Service Security refers to the mechanisms and processes used to verify the identity of a user before granting access to mobile devices, applications, or wireless services. It is a critical component in protecting sensitive data and preventing unauthorized access in mobile and wireless computing environments.

Authentication Methods

1. **Password / PIN-based Authentication**
   Users authenticate using a secret password or personal identification number.
2. **One-Time Password (OTP)**
   A temporary password sent via SMS, email, or authentication apps, valid for a short duration.
3. **Biometric Authentication**
   Uses physical or behavioral traits such as fingerprint, face recognition, iris scan, or voice recognition.
4. **Two-Factor / Multi-Factor Authentication (2FA/MFA)**
   Combines two or more authentication factors to enhance security.

Security Challenges

- Use of weak or reused passwords
- OTP interception through malware or SIM swapping
- Spoofing of biometric data
- Replay and impersonation attacks

Conclusion : Authentication service security plays a vital role in safeguarding mobile and wireless systems. Strong authentication mechanisms and proper security practices help reduce cyber threats and ensure secure access to mobile services.

Attacks on Mobile / Cell Phones

Mobile or cell phones are highly vulnerable to cyberattacks because they store personal, financial, and sensitive information and are constantly connected to wireless networks. Cybercriminals exploit security weaknesses in mobile devices to steal data, commit fraud, or disrupt services.

Common Attacks on Mobile / Cell Phones

1. **Malware Attacks**
   Malicious software such as viruses, worms, Trojans, and spyware infect mobile devices to steal data, track activities, or damage the system.
2. **Smishing (SMS Phishing)**
   Fraudulent text messages trick users into revealing passwords, OTPs, or bank details.
3. **Malicious Applications**
   Fake or unauthorized apps installed from untrusted sources steal personal and financial information.
4. **Bluetooth Attacks**
   Attackers exploit unsecured Bluetooth connections to access files or control the device.
5. **Wi-Fi Attacks**
   Using public or unsecured Wi-Fi networks enables man-in-the-middle attacks and data interception.
6. **SIM Swapping Attacks**
   Criminals gain control of a victim's mobile number to receive OTPs and reset account credentials.
7. **Denial of Service (DoS) Attacks**
   The device is flooded with requests, causing it to slow down or become unusable.
8. **Physical Attacks**
   Loss or theft of mobile phones leading to unauthorized access to data.

Prevention Measures

- Install apps only from trusted sources
- Avoid clicking unknown links or messages
- Use strong authentication and device locks
- Keep the operating system updated
- Avoid public Wi-Fi for sensitive transactions

Conclusion

Attacks on mobile and cell phones pose serious security and privacy risks. Proper security measures, user awareness, and safe mobile usage practices are essential to protect against these threats.

Mobile Devices: Security Implications for Organizations

Mobile devices, including smartphones, tablets, and laptops, bring flexibility and productivity but also introduce significant security risks:

Security Implications

1. **Data Breaches and Leakage**
   - Sensitive corporate data can be accessed if devices are lost, stolen, or compromised.
2. **Malware and Phishing Attacks**
   - Mobile malware can spread through apps, emails, or malicious websites.
3. **Unsecured Networks**
   - Public Wi-Fi or unencrypted connections increase the risk of interception.
4. **Device Theft and Loss**
   - Physical theft of devices can expose confidential information.
5. **BYOD (Bring Your Own Device) Risks**
   - Personal devices may not meet organizational security standards.
6. **Application Vulnerabilities**
   - Unauthorized apps can access organizational data without permission.
7. **Insider Threats**
   - Employees with malicious intent or negligence can compromise security.

Mitigation Strategies:

- Use Mobile Device Management (MDM) solutions.
- Require strong passwords, multi-factor authentication, and regular updates.
- Educate employees on safe device usage.
- Encrypt sensitive data and control access.
- Monitor personal device and app usage.

Conclusion: Organizations must implement strong mobile security measures to protect sensitive data and reduce potential threats.

Organizational Measures for Handling Mobile Device-Related Security Issues

Organizations must adopt proactive measures to mitigate mobile security risks:

Technical Measures

1. **Mobile Device Management (MDM)**
   - Centralized control over device configuration, updates, and security enforcement.
2. **Encryption**
   - Encrypt sensitive data on devices and during transmission.
3. **Secure Access**
   - Use VPNs, multi-factor authentication (MFA), and secure Wi-Fi.
4. **App Control**
   - Whitelist approved applications; block unauthorized apps.

5. **Remote Wipe**
    - Ability to erase data from lost or stolen devices.
6. **Patch Management**
    - Ensure timely updates to OS and apps to fix vulnerabilities.

Administrative Measures

1. **Employee Training**
    - Educate staff about mobile security best practices and phishing threats.
2. **BYOD Policy**
    - Define guidelines for personal devices accessing corporate networks.
3. **Regular Audits**
    - Periodic checks for compliance with mobile security policies.
4. **Incident Response Plan**
    - Procedures to handle mobile security incidents quickly and effectively.

Conclusion:

By implementing these measures, organizations can significantly reduce mobile device-related security risks while supporting efficient and secure mobile work environments.

Organizational Security Policies and Measures in the Mobile Computing Era

In the mobile computing era, organizations need comprehensive policies:

Policy Components

1. **Acceptable Use Policy**
    - Guidelines on appropriate device usage and data handling.
2. **Access Control Policy**
    - Define user privileges and authentication requirements.
3. **Data Classification and Handling**
    - Identify confidential, internal, and public data; implement protection accordingly.
4. **Device Management Policy**
    - Registration, monitoring, and removal of mobile devices.
5. **Software and Patch Policy**
    - Standardization and update requirements for apps and OS.

Measures

- **Zero Trust Security Model:** Verify every access request before granting access.
- **Network Segmentation:** Separate sensitive systems from general mobile device access.
- **Continuous Monitoring:** Detect unusual device behavior or potential breaches in real-time.

Conclusion:

Effective security policies and measures enable organizations to harness mobile computing benefits while minimizing risks.

Laptops: Mobile Security Considerations

Although laptops are traditional mobile devices, they present specific risks:

1. **Physical Security**
   - Risk of theft or loss; use cable locks or secure storage.
2. **Data Encryption**
   - Full disk encryption for sensitive corporate data.
3. **Secure Boot & BIOS Protection**
   - Prevent malware from loading at startup.
4. **Remote Management**
   - Ability to track, lock, or wipe a laptop remotely.
5. **Antivirus & Endpoint Protection**
   - Install and regularly update antivirus software.
6. **User Awareness**
   - Encourage strong passwords, screen locks, and cautious browsing habits.

Conclusion:

Proper security measures for laptops are essential to protect organizational data and maintain operational continuity in mobile work environments.

UNIT-III:

Tools and Methods Used in Cybercrime: Password Cracking, key loggers and Spywares, virus and worms, Trojan Horses and Backdoors, Steganography, attacks on wireless networks, Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft).

UNIT-III:

Cybercriminals use various **tools and techniques** to steal data, hack systems, and commit fraud. Below are some of the most **common cybercrime methods** and how to protect yourself.

Password Cracking:

Hackers steal or guess passwords to access personal and business accounts.

Common Methods:

- **Brute Force Attack:** Tries every possible password combination.
- **Dictionary Attack:** Uses a list of common passwords.
- **Credential Stuffing:** Uses stolen passwords from one site to access another.

How to Stay Safe:

✔Use **strong, unique passwords** (e.g., mix letters, numbers, symbols).

✔Enable **Two-Factor Authentication (2FA)**.

✔Change passwords **regularly**.

Keyloggers & Spyware

Malicious programs secretly record your keystrokes and spy on your activities.

How Hackers Use It:

- Installed via fake software, phishing emails, or infected USB devices.
- Steals usernames, passwords, credit card details, and private messages.

How to Stay Safe:

✔Install **antivirus software** and update it regularly.

✔Avoid downloading software from unknown sources.

✔Use **virtual keyboards** for sensitive data entry.

Viruses & Worms

Self-spreading malware that infects files or networks.

Differences:

- **Virus:** Needs user action (like opening an infected file) to spread.
- **Worm:** Spreads automatically across networks without user interaction.

How to Stay Safe:

✔Avoid opening **suspicious email attachments**.

✔Keep your **OS and apps updated**.

✔Install **firewalls and antivirus software**.

Trojan Horses & Backdoors

Malicious software disguised as a legitimate app.

How Hackers Use It:

- **Trojan Horse:** A fake app that looks safe but installs malware.
- **Backdoor:** Secret access to a system, allowing hackers to control it remotely.

How to Stay Safe:

✔Download apps only from **official sources**.

✔Use **security software** to detect Trojans.

✔Never install software from **unknown links**.

Steganography

Hiding secret data inside files, images, or videos.

How Hackers Use It:

- Hide **malware inside images or videos**.
- Steal **confidential data without detection**.

How to Stay Safe:

✔Be cautious when downloading **media files from unknown sources**.

✔Use **cybersecurity tools** that detect hidden malware.

Attacks on Wireless Networks

Hackers target Wi-Fi networks to steal data or gain unauthorized access.

Common Wireless Attacks:

- **Evil Twin Attack:** Fake Wi-Fi that looks like a real one to steal your data.
- **Man-in-the-Middle (MitM):** Hackers intercept your data on public Wi-Fi.
- **Wi-Fi Cracking:** Hackers break weak passwords to access networks.

How to Stay Safe:

✔Use **strong Wi-Fi passwords** and **WPA3 encryption**.

✔Avoid connecting to **public Wi-Fi without a VPN**.

✔Disable **automatic Wi-Fi connections**.

Phishing & Identity Theft

Phishing:

Phishing is a cyberattack where hackers **pretend to be a trusted source** (like a bank, company, or government) to steal login details, credit card info, or personal data.

Common Types of Phishing:

 Email Phishing – Fake emails ask you to click on a link and enter your details.
 Smishing (SMS Phishing) – Fake text messages trick you into clicking malicious links.
 Vishing (Voice Phishing) – Fraudsters call pretending to be from your bank or tech support.
 Spear Phishing – Targeted attacks on individuals (e.g., company executives).
 Website Phishing – Fake websites look like real ones to steal login details.

How to Stay Safe from Phishing:

✔**Don’t click on suspicious links or attachments.**

✔**Check email senders carefully** for misspelled domains (e.g., "g00gle.com" instead of "google.com").

✔**Never share passwords or banking details via email or phone.**

✔**Enable Two-Factor Authentication (2FA)** to add extra security.

✔**Verify links before clicking** (hover over them to see the real URL).

Identity Theft (ID Theft)

Identity Theft: Identity theft happens when criminals **steal personal information** (like name, SSN, or credit card details) to commit fraud or impersonation.

 Common Ways Hackers Steal Identities:

- **Phishing Attacks** – Tricking victims into sharing sensitive details.
- **Data Breaches** – Hacking companies and leaking user information.
- **SIM Swapping** – Hijacking your phone number to reset passwords.
- **Skimming** – Stealing credit card info via fake ATMs or payment terminals.
- **Social Engineering** – Manipulating victims to reveal personal data.

✅**How to Protect Yourself from ID Theft:**

✔**Use strong, unique passwords** for all accounts.

✔**Enable 2FA** to protect important accounts.

✔**Monitor your bank and credit card statements** for suspicious transactions.

✔**Avoid sharing personal details on social media.**

✔**Shred personal documents** before disposing of them.

✔**Use credit monitoring services** to detect unusual activity.